UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/613,911	07/05/2003	Alexander Medvinsky	018926-010400US	4648

43471	7590	07/19/2006		EXAMINER

GENERAL INSTRUMENT CORPORATION DBA THE CONNECTED
HOME SOLUTIONS BUSINESS OF MOTOROLA, INC.
101 TOURNAMENT DRIVE
HORSHAM, PA 19044

HOFFMAN, BRANDON S

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 07/19/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

	Application No.	Applicant(s)
Office Action Summary	10/613,911	MEDVINSKY, ALEXANDER
	Examiner	Art Unit	
	Brandon S. Hoffman	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>22 May 2006</u>.

2a)☒ This action is **FINAL**.   2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>1 and 3-10</u> is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) <u>1 and 3-10</u> is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
    Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____.

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

1.   Claims 1 and 3-10 are pending in this office action.

2.   Applicant's arguments, filed May 22, 2006, have been fully considered but they
are not persuasive.

Rejections

3.   The text of those sections of Title 35, U.S. Code not included in this action can
be found in a prior Office action.

Claim Rejections - 35 USC § 103

4.   Claims 1 and 3-10 are rejected under 35 U.S.C. 103(a) as being unpatentable
over Neuman et al. (Kerberos: An Authentication Service for Computer Networks,
published September 1994) in view of Rich et al. (U.S. Patent Pub. No. 2002/0078243).

        Regarding claim 1, Neuman et al. teaches a method for providing a secure time
signal from a time source to a time requestor over a digital network, the method
comprising:

- Sending a requestor identification to an authentication server (page 5,
  AUTHENTICATION REQUEST AND REPONSE, first paragraph, and page 4,
  figure 1, steps 1 and 2);

- Receiving a public key from the authentication server (page 10, PUBLIC-KEY CRYPTOGRAPHY, last paragraph);

- Sending a request for a time server ticket (page 4, APPLICATION REQUEST AND RESPONSE, first paragraph, and page 6, figure 2, step 3);

- Receiving the request for the time server ticket (page 4, APPLICATION REQUEST AND RESPONSE, first paragraph, and page 6, figure 2, step 4); and

- Using **the** time server ticket to request the secure time signal wherein the time server ticket includes an identification of the requestor and a session key for transferring the secure time signal (page 3 and 4, THE KERBEROS TICKET, both paragraphs, and page 6, figure 2, step 5).

Neuman et al. does not specifically teach a time server ticket for obtaining a secure time signal. However, Neuman et al. teaches Kerberos, and more specifically, a ticket granting server for obtaining verification for a client to prove they are who they say they are without having to send further data over the network that could be used to impersonate the client at a later time (page 2, THE KERBEROS AUTHENTICATION SERVICE).

Rich et al. teaches the utilization of time server tickets (paragraph 0034 and 0045).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine time server tickets, as taught by <u>Rich et al.</u> with the apparatus/medium of <u>Neuman et al.</u> It would have been obvious for such modifications because Kerberos has the drawbacks of assuming the clocks of clients are correct. By utilizing time server tickets, correct times can be ensured to prevent replay attacks (see paragraph 0006-0008 of Rich et al.).

Regarding <u>claims 3-5</u>, the combination of <u>Neuman et al.</u> in view of <u>Rich et al.</u> teaches wherein the time server ticket is obtained from a key distribution center, from an authentication server, or from a ticket-granting-server (see page 6, figure 2, AS and TGS of Neuman et al.).

Regarding <u>claim 6</u>, the combination of <u>Neuman et al.</u> in view of <u>Rich et al.</u> teaches further comprising: transferring the time server ticket with a request for a secure time signal to a secure time server; and receiving the secure time signal from the secure time server (see page 3 and 4, THE KERBEROS TICKET, both paragraphs, and page 6, figure 2, steps 5 and 6 of Neuman et al. and paragraph 0034 & 0045 of Rich et al.).

Regarding <u>claim 7</u>, the combination of <u>Neuman et al.</u> in view of <u>Rich et al.</u> teaches wherein the request includes a request message, the method further comprising: generating a nonce to be included in the request message; including a session key for the secure time server in the request message; and including a keyed

checksum over the request message (see page 4, APPLICATION REQUEST AND

RESPONSE, first paragraph, and page 5, AUTHENTICATION REQUEST AND

RESPONSE, first paragraph of Neuman et al.).

Regarding claim 8, the combination of Neuman et al. in view of Rich et al.

teaches wherein the secure time signal includes a reply message, the method further

comprising: including the nonce copied from the request in the reply message; and

including a keyed checksum over the reply message (see page 4, APPLICATION

REQUEST AND RESPONSE, second paragraph, and page 5, AUTHENTICATION

REQUEST AND RESPONSE, second paragraph of Neuman et al.).

Regarding claim 9, the combination of Neuman et al. in view of Rich et al.

teaches wherein the step of receiving a secure time signal includes the following:

matching the nonce in the reply message with the corresponding nonce in the request

message; and confirming the keyed checksum (see page 4, APPLICATION REQUEST

AND RESPONSE, second paragraph of Neuman et al.).

Regarding claim 10, the combination of Neuman et al. in view of Rich et al.

teaches further comprising using the secure time signal to update a clock value (see fig.

7, ref. num 714/716/718 of Rich et al.).

Response to Arguments

5.   Applicant argues the combination of references does not teach a time server

ticket (page 6 through page7).

        Regarding applicant's argument, examiner disagrees. Applicant admits that Rich

et al. teaches receiving time synchronization information from a key distribution center

(KDC) server (see page 7, first paragraph of applicant's remarks). Examiner agrees

with applicant. This clearly shows, combined with the limitation of claim 3, that a KDC

server is responsible for receiving a request for a time server ticket and responding with

a time server ticket to the requestor.

Conclusion

6.   **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time

policy as set forth in 37 CFR 1.136(a).

        A shortened statutory period for reply to this final action is set to expire THREE

MONTHS from the mailing date of this action. In the event a first reply is filed within

TWO MONTHS of the mailing date of this final action and the advisory action is not

mailed until after the end of the THREE-MONTH shortened statutory period, then the

shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later

than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Brandon S. Hoffman whose telephone number is 571-272-3863. The examiner can normally be reached on M-F 8:30 - 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

BH

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100